基于区块链技术的信息网络安全防护体系构建与优化

杜刚
黑龙江大学，黑龙江 哈尔滨 150008
DOI: 10.61369/TACS.2025010031

摘　　要： 互联网技术以迅雷不及掩耳之势渗透进各行各业发展中，对信息网络安全带来了不小的挑战，尤其对用户数据安全、网络信任机制和系统安全造成了威胁。区块链技术具有去中心化、不可篡改和共识性强等优点，为构建信息网络安全防护体系提供了新的技术支持。本文分析了传统网络安全防护体系核心缺陷，明确了区块链技术在信息网络 安全防护体系中的优势，提出要优化体系架构设计、明确关键技术模块、改进 PBFT 共识算法、开启分布式身份认证、智能合约安全验证，实时动态访问控制，从而全面提高信息网络安全防护能力。

关 键 词： 区块链技术；信息网络安全；防护体系；共识机制；智能合约

Construction and Optimization of Information Network Security Protection System Based on Blockchain Technology

Du Gang
Heilongjiang University, Harbin, Heilongjiang 150008

Abstract: Internet technology has penetrated into the development of various industries at an overwhelming speed, posing significant challenges to information network security. It particularly threatens user data security, the network trust mechanism, and system security. Blockchain technology, with its advantages of decentralization, immutability, and strong consensus, provides new technical support for constructing an information network security protection system. This article analyzes the core defects of traditional network security protection systems, clarifies the advantages of blockchain technology in information network security protection systems, and proposes measures such as optimizing the system architecture design, defining key technical modules, improving the PBFT consensus algorithm, enabling distributed identity authentication, conducting smart contract security verification, and implementing real – time dynamic access control, so as to comprehensively enhance the information network security protection capabilities.

Keywords: blockchain technology; information network security; protection system; consensus mechanism; smart contract

引言

数字经济时代下，信息网络成为数字金融、社会治理、企业管理的核心技术之一，应用范围越来越广泛，带来的网络安全威胁也趋向于多元化、复杂化。据《2024年全球网络安全报告》显示，全球每年因网络攻击导致的经济损失超过6万亿美元，如何提高网络安全防护能力成为计算机领域研究热点。随着计算机病毒、网络攻击技术不断升级迭代，传统安全防护技术在预防数据篡改、识别身份伪造和地域分布式（DDoS）攻击等方面逐步实效。基于此，区块链技术逐步成为信息网络安全防护的核心技术之一，有效应对分布式拒绝服务（DDoS）攻击，直接进行可信数据交互，通过智能化算法识别用户身份，解决网络安全防护体系中的“信任孤岛”和“单点故障”问题。

本文分析了区块链技术在信息网络安全防护中的应用优势、应用策略，明确区块链技术在信息网络安全防护体系中的基础设施层、中间件层和应用中的应用，阐述 PBFT 共识算法优化、智能合约动态更新机制和隐私数据保护方式，为信息网络安全防护体系研发提供参考。

一、传统信息网络安全防护体系的缺陷分析

（一）中心化架构的单点风险

传统网络安全体系采用中心化管理模式，通过集中式认证服务器、单一防火墙和统一日志进行安全防护。这种安全防护体系存在很大弊端，一旦防护体系中心节点被黑客攻破或感染计算机病毒，整个安全防护体系就会瘫痪，容易导致用户计算机数据丢失，带来难以挽回的损失[1]。

（二）数据完整性保护机制的局限性

在传统网络安全防护体系中，数字签名技术、哈希校验是维护数据完整性的主要技术，通过中心化数据库储存和验证数据，一旦攻击者篡改中心数据库记录、伪造数字签名，容易导致系统数据被窃取或篡改，威胁用户数据安全、资金安全。此外，在进行跨系统数据交互时，不同系统采用的数据库不同，存在数据信任壁垒，难以实现数据共享、数据安全验证。

（三）动态信任机制的缺失

计算机网络运行过程中会产生大量数据，需要安全防护体系实施动态化防护，但是传统网络安全防护体系采用静态权限，无法根据实时网络动态调整信任等级，难以及时发现系统运行过程中存在的安全漏洞、外部攻击，威胁了系统安全[2]。传统安全防护体系缺少自动化信任评估、响应机制，无法根据实时监测到的网络威胁调整信任等级，导致 APT 攻击监测时间过长，影响了网络安全防护体系运行。

二、区块链技术在网络安全防护中的核心优势

（一）去中心化架构增强系统稳定性

区块链采用分布式节点网络，具有去中心化特征，各个节点可以独立存储数据、执行共识算法，即使某个节点被攻击，其他节点也可以顺利运行，从而保证整个计算机网络系统顺利运行。区块链去中心化结构可以显著提升网络安全防护体系稳定性，各个节点之间不会制约，每个节点可以独立存储数据，即使某个节点遭受攻击、感染计算机病毒，其他节点也可以保证整个安全防护体系的运转，从而提高安全防护体系抗攻击能力[3]。

（二）不可篡改特性保障数据完整性

区块链采用密码学哈希链技术存储数据，每一个节点都包含前一个节点的哈希值，形成不可逆的链式结构，确保整个安全防护体系数据的完整性。链式结构上的数据彼此之间联系紧密，任何一个数据的修改都需要通过整个系统共识节点的验证，只有通过验证后才可以修改数据，从而有效杜绝安全防护体系数据被篡改或伪造的可能。

（三）智能合约实现自动化信任机制

智能合约是区块链运行过程中的可编程代码，根据预设算法、程序自动执行合约条款，自动对系统运行过程中的访客权限、数据存储等进行验证，从而建立自动化信任机制。在智能合约技术支持下，区块链可以帮助网络安全体系实现动态访问控制，一旦检测到系统数据异常、外部攻击时，可以自动开启权限降级或隔离，保证系统顺利运行[4]。对系统数据共享过程进行动态监测，根据实时信任评分自动调整数据访问、下载和传输权限，保证安全防护体系数据共享的安全性。

（四）分布式共识构建可信协作环境

区块链采用 POW、POS、PBFT 共识机制，确保各个分部节点数据动态保持一致，让各个节点之间建立信任机制，营造可信协作环境，提高系统安全防护性能。在跨机构网络中，各参与方通过区块链技术参与系统管理，通过公示算法、分布式节点建立可信账本，实现安全数据共享、协同审计，从而提高安全防护体系抵御风险的能力[5]。

三、基于区块链的信息网络安全防护体系构建

（一）体系架构设计

1. 基础设施层：分布式信任底座

分布式身份认证（DID）：信息网络安全防护体系采用区块链分布式身份系统，利用加密哈希值存储用户信息，并把用户信息存储在区块链链式结构上，通过零知识证明技术进行身份验证，避免用户数据泄露或被篡改[6]。例如信息网络安全防护体系可以开启用户年龄限制，要求注册用户年满18周岁，无需用户上传具体的出生年月信息，仅需用户提交年龄证明即可，通过智能合约进行验证，便于用户操作、保障用户数据安全。

共识节点部署：根据用户安全防护需求、网络规模来部署区块链共识节点，采用 PBFT 或改进的 DPoS 算法，明确各个节点共识原则、数据共享程序，从而数据共享。例如在企业内网中，可以采用许可链架构，针对各个节点设置身份认证要求，只有通过身份认证后才可以加入内网，各个节点数据独立存储，即使某个节点受到攻击、数据被篡改，整个信息网络安全防护体系也可以顺利运行。

2. 中间件层：智能安全策略引擎

动态访问控制模块：基于智能合约技术支持，网络安全防护体系可以建立访问控制数据库，明确用户权限等级、设备终端安全等级、时间窗口、身份认证等参数，开展智能安全防护，提高系统防御能力[7]。一旦用户向系统发送访问请求时，智能合约可以自动调取区块链各个节点上的实时数据，例如系统安全漏洞修复记录、用户访问和资源下载记录，计算该用户信任评分，从而自动调整用户访问权限，从而实现智能控制访问权限。

入侵检测与响应模块：在网络安全防护体系中部署分布式 IDS/IPS 系统，将各个节点检测到的可疑数据上传到区块链上，通过智能合约把这些可疑数据和链上的攻击特征库数据进行对比。一旦发现可疑数据与攻击特征库数据相同或高度疑似，可以自动触发跨节点预警，封禁攻击源 IP、隔离受感染的节点和移动终端设备，并把本次攻击事件、可疑数据记录在审计链上，杜绝后续再次遭受相似攻击[8]。

3. 应用层：全场景安全防护

数据安全共享：医疗、金融等机构网络安全防护要求比较高，可以搭建联盟链，满足医疗、金融跨机构数据共享需求，根据机构需求对数据进行加密处理，把加密数据哈希值上链，当检测到需求方访问申请后，智能合约对其账户权限进行审核，并生成临时解密密钥，实时记录密钥使用记录、数据访问和操作记录，确保后续数据流向可以精准追溯。

安全审计与溯源：构建独立的审计区块链，自动采集系统运行过程中的操作日志、数据库、策略调整等数据，对各个节点数

据进行审计，确保数据不会被篡改。

（二）关键技术模块实现

1. 改进的 PBFT 共识算法优化

本文提出基于分组的分层 PBFT（HPBFT）算法，把信息网络安全防护体系中的各个节点划分为若干个小组，明确每个小组的主节点、组内共识，再在主节点上形成上层共识网络，利用分层 PBFT 算法对每层数据进行审核与监管。

2. 零知识证明与同态加密结合的隐私保护

基于区块链的信息网络安全防护体系采用零知识证明技术、同态加密技术保护用户隐私，重点对系统内用户身份认证、数据共享过程进行监管，隐藏用户敏感信息，并对数据传输、共享过程进行同态加密处理。例如，用户向服务器发出“访问某文件”请求时，只需要根据用户在区块链上的权限合约的哈希值进行验证即可，不涉及对用户隐私数据的传输，从而保证用户隐私数据安全。

3. 智能合约动态更新机制

为解决智能合约漏洞问题，信息网络安全防护体系可以采用“沙箱测试 – 多签审批 – 灰度部署”的动态管理流程。新合约版本首先在隔离环境中进行形式化验证和攻击模拟测试，通过后需至少3/4的管理节点多重签名确认，再逐步部署到部分节点进行灰度测试，最终全网同步更新，确保策略调整的安全性和可靠性。

四、基于区块链技术的信息网络安全防护体系优化策略

（一）性能优化策略

跨链协同机制：针对复杂网络中多区块链并存的场景，引入跨链技术（如哈希锁定、公证人机制）实现不同链间的安全数据交互。例如，企业内部业务链与审计链通过跨链接口同步关键数据，既保证业务链的高效运行，又满足审计链的监管需求[9]。

轻节点技术应用：在资源受限的物联网设备中部署轻节点，仅存储区块信息而非完整账本，通过向全节点请求证明来验证交易合法性，降低设备存储和计算负担，使区块链技术可扩展至边缘计算场景。

（二）安全性增强策略

量子抗性优化：随着量子计算技术的发展，传统加密算法面临破解风险。在区块链底层引入抗量子密码算法（如格密码、哈希签名），对私钥生成、交易签名等关键环节进行升级，确保体系在量子计算环境下的安全性[10]。

动态蜜罐诱捕系统：在区块链节点中嵌入智能蜜罐，当检测到异常连接请求时，自动生成虚假交易数据和节点地址，引导攻击者进入隔离的蜜罐网络，同时将攻击特征上链共享，实现全网协同的主动防御。

五、挑战与未来研究方向

（一）现存挑战

性能与扩展性：尽管改进的共识算法提升了效率，但区块链的 TPS（每秒交易处理量）仍低于中心化系统，需进一步研究分片技术、二层网络（如闪电网络）在安全防护中的应用。

监管与合规：区块链的去中心化特性与数据主权监管存在潜在冲突，需探索“监管节点”机制，在保证安全性的同时满足合规要求。

跨代技术融合：5G、物联网、人工智能与区块链的深度融合面临协议不兼容、安全边界模糊等问题，需构建跨技术领域的协同防护框架。

（二）未来研究方向

AI 驱动的智能合约审计：利用机器学习技术自动识别合约漏洞，结合形式化验证构建全方位的合约安全检测体系；

自进化安全体系：通过区块链记录安全事件和防护策略，利用联邦学习实现全网安全知识共享，使系统具备自我优化和威胁预测能力；

标准化建设：推动区块链安全技术标准制定，包括数据上链规范、共识算法安全评估、跨链互操作协议等，促进技术落地和产业协同。

六、结论

本文构建的基于区块链技术的信息网络安全防护体系，通过去中心化架构、智能合约自动化和分布式共识机制，有效解决了传统体系的单点风险、信任壁垒和动态响应不足问题。实证分析表明，该体系在数据安全、抗攻击能力和协作效率上具有显著优势，为网络安全防护提供了可落地的技术方案。未来需进一步突破性能瓶颈，加强跨技术融合和标准化建设，推动区块链技术在关键信息基础设施保护中的规模化应用。

参考文献

[1] 李明，王芳 . 区块链技术在网络安全中的应用研究 [J]. 信息安全学报 ,2023,8(3):45-53.

[2] 顾丽旺，梁娜，初晓翠，等 . 基于区块链技术的互联网信息安全思路探索 [J]. 网络安全技术与应用 ,2023,(10):16-18.

[3] 彭青梅 . 基于区块链技术的网络信息安全管理系统设计 [J]. 信息记录材料 ,2024,25(4):110-112.

[4] 梁娜，李修倩，丁宜鹏，等 . 基于区块链的分布式网络安全防护架构设计 [J]. 软件 ,2024,45(12):180-182.

[5] 张铠，黄晋，汪希 . 基于区块链技术的网络信息安全访问控制方法 [J]. 信息技术与信息化 ,2024,(09):197-200.

[6] 崔馨月 . 基于大数据区块链的网络安全防护系统研究 [J]. 网络空间安全 ,2024,15(04):248-251.

[7] 刘斯远，王博琼 . 基于区块链技术的网络用户隐私信息安全防护研究 [J]. 信息记录材料 ,2024,25(01):20-22.

[8] 谭小伟 . 基于区块链技术的网络信息安全防护与应用 [J]. 电脑知识与技术 ,2023,19(32):78-80.

[9] 詹冰 . 基于区块链的网络隐私数据安全防护模型设计 [J]. 信息与电脑（理论版）,2022,34(24):219-221.

[10] 韩阳，石颖 . 局域网环境下计算机网络安全防护技术应用研究 [J]. 中国新通信 ,2022,24(16):113-115.

